Los Alamos
NATIONAL LABORATORY
EST.1943

LA-UR-18-31541
Approved for public release; distribution is unlimited.

Title: Cyber Science Capability Strategy

Author(s): Pratt, Rebecca Lynn; Kirkland, Matt W.; Fisk, Michael Edward; Breiner, Carla Kay; Dendy, Edward Dwight; Dors, Eric Edward; Funsten, Herbert O.; Humbert, William Rowland; Meyerhofer, David Dietrich; Shlachter, Jack S.; Zollinger, Michael S.

Intended for: Internal Document

Issued: 2018-12-11

Disclaimer:
Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by Triad National Security, LLC for the National Nuclear Security Administration of U.S. Department of Energy under contract 89233218CNA000001. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

2018

Cyber Science Capability Strategy

Rebecca L Pratt (A-4)

LANL CYBER DOMAIN INTERNAL INVESTMENT PRIORITIES

FISK, M (OCIO & CHAIR), BREINER, C (WRS-DO), DENDY, E (CCS-DO), DORS, E (GS-IET), FUNSTEN, H (ISR-DO), HUMBERT, W (GS-NSD), KIRKLAND, M (A-DO), MEYERHOFER, D (P-DO), SHLACTER, J (T-DO), ZOLLINGER, M (NIE-DO)

September 13, 2018

Cyber Science Capability Strategy

Los Alamos National Laboratory

Vision

Become recognized as one of the top research and development national laboratories for cyber resilience in national security systems.

We aim to reach this vision through strategic and multi-disciplinary investments in cyber capabilities including artificial intelligence, information integrity, defensible and resilient complex system design, and post-quantum security.

Scope & Objective

This document outlines LANL's cyber science capability strategy, working in tandem with the IS&T strategy, to focus internal investments utilizing our unique skill sets, capabilities and facilities supporting national scientific priorities to address emerging challenges to national security. This strategy identifies LANL's strengths as they relate to cyber science and is intended to guide internal investments to increase the strength, focus, and impact of LANL's cyber capability building innovative scientific leadership. Subsequent documents (human capital development, implementation, capabilities, infrastructure, etc.) will develop plans targeting specific program areas including weapons, energy, and strategic partnership programs.

Motivation

In February 2016 President Obama identified cybersecurity as one of the nation's most pressing challenges. In May 2017 President Trump issued an Executive Order on Cyber focusing on managing cyber risk followed by Secretary Perry listing high performance computing and cyber as two of the top three priorities for the Department of Energy. Several cyber agencies are being elevated, including USCYBERCOM and DOE's new Assistant Secretary and Office of Cybersecurity, Energy Security, and Emergency Response (CESER). In July 2018, the Executive Office of the President issued the FY2020 Administration Research and Development (R&D) budget priorities that included artificial intelligence (AI), machine learning, quantum computing, cyber capabilities, science to improve the security and resilience of critical infrastructure and modernizing R&D infrastructure.

This cyber science capability strategy is to focus efforts and investments in people, facilities, research, program development, and operational cyber sciences to enable and support the following capabilities over the next 3-5 years. A component of this investment must include the instrumentation and augmentation of existing facilities to create end-to-end testbeds that generate the data sets and realistic scenarios to develop, exercise and test these capabilities in mission-relevant environments. Prime candidates are the local electrical grid and weapons engineering, physics and production systems. These candidates include significant operational technology (OT), a key differentiator that leverages unique LANL capabilities and mission experience.

Directed Capability Development Investments

Artificial Intelligence (AI). Since the 1980s LANL has developed a series of practical systems (including Wisdom & Sense, NADIR, EMAAD/NARQ, PathScan, CodeVision, and REDUCE) that use expert systems, machine learning, reverse engineering, and predictive statistical models to identify suspicious activity in complex system event data and in executables and content. These systems continue to have academic, government, and commercial impact.

Emerging and contemporary concerns include adversarial machine learning (e.g. automated cyber-attacks) and quantifying and improving the bounds of detection for malicious activity. The volume, velocity, and veracity of the data that may be used to identify and respond to an attack on large, national-scale networks make this a "big data" problem and exercise data management and data-intensive supercomputing (DISC). Modern, large-scale analytics platforms are a prerequisite for this work, to include neuromorphic computing capabilities.

Like many Science of Signatures problems, the quality of analytics relies on advances in data collection and the design and engineering of domain-and system-specific sensors such as those for mobile, manufacturing, industrial control, grid, airborne, space, and weapons systems. Beyond the mathematical analysis of data, this thrust includes the challenges of human computer interaction for analytics, presenting data in meaningful context, and providing situational awareness and enabling specific, targeted, automatic response actions. Embedded in this topic area, and linked to Information Integrity, is the need to be resilient to and enhance detection of false or unsubstantiated information from overt or covert data streams that could include physical sensing, and that lead to undesired alterations in ML/AI responses/behaviors.

Defensible and Resilient Complex System Design. Design of inherently robust systems, explicitly intended for use in an adversarial environment, that enables the quantification of the ability of systems to retain mission assurance or intrusion tolerance, maintain security or robustness properties as the result of attacks, vulnerabilities, or design changes. Applications could include resiliency for system of systems involving critical sensing platforms (terrestrial or space) and associated data networks, data processing and decision support systems, power grid, nuclear command & control and weapon design and production. This topic area overlaps with AI and Information Integrity capability areas.

Post-Quantum Security. Worldwide progress in quantum information science (QIS) is accelerating rapidly, not least because of recent large investments (>$10 Bn) announced in China. LANL will leverage its existing strength in QIS to be at the forefront of quantum computing science for national security applications. In addition, LANL's diverse teams of theoretical and experimental physicists and mathematicians are uniquely positioned to develop and assess data assurance methods that remain strong even after an adversary develops quantum computing. As quantum communication systems enter daily use worldwide LANL will lead the way in understanding and taking advantage of these systems' strengths and weaknesses.

Information Integrity. As machine learning in the cyber domain is given agency in the physical world, the threat of adversarial information attack on autonomous systems makes it is easy to imagine that the possibility of forcing autonomous, machine learning systems to undesirably behave as physical extensions of the adversarial entity. Even absent a machine learning system to make basic decisions, human operators may similarly respond incorrectly to spoofed data designed to stimulate the unwitting facilitation of adversarial actions. The challenge becomes even more difficult if the false or unsubstantiated data used in an information attack is used to challenge an artificial intelligence entity that operates beyond a learned training, and extrapolates to solutions outside of its previous experience when faced with new or inconsistent data. This challenge necessarily synthesizes research in the other three investment areas: Artificial Intelligence, Defensive and Resilient Complex System Design and Post-Quantum Security, but is focused on data resiliency.

Interdisciplinary Approach

A new era of information warfare is taking place on cyber-physical systems composed of distributed computers and processing systems connected by network infrastructure that performs physical actions in the real world. Security threats to these complex cyber-physical systems take place on many levels including sensors, information

processing components, cyber-coupled operational technology control systems, and physical actuators. Countering these threats requires understanding, models, and data that span the entire system. LANL should take a scalable and sustainable approach that is aligned with the laboratory's scientific foundation by encouraging the creation of interdisciplinary teams that pair cyber sciences domain experts with theoretical and experimental scientists to develop innovative research results and solutions. This approach to teaming ensures that LANL's scientific strengths are informed by established mission opportunities.

Although the mission requirements vary widely, cyber-physical systems share the properties of real-time sensing, sense-making, and control or decisions in the presence of uncertainty. As cyber systems are emerging and changing at a rapid rate, application-focused investment may yield quickly outdated solutions. LANL's Cyber Science Strategy guides investment toward critical capabilities that address emerging opportunities to provide information confidentiality and integrity, while ensuring system availability and mission performance.

Existing Capability areas that support Directed Capability Development Investments include:

- Eliminating information uncertainty through provable security of the future:
    - Quantum Communications/Computing: Los Alamos leads the weapons complex in quantum information science and its applications to national security needs. LANL technical efforts cover the full range from basic research in quantum science to development of deployed systems to commercialization of quantum-enabled security products.
    - Experimental and theoretical physics and applied mathematics come together to study the potential of quantum computation to solve otherwise intractable problems; to develop novel sensors with unprecedented sensitivity, and to provide secure communication algorithms based on quantum principles
- Multi-system/network data science, adversary detection and defense:
    - Complex System Modeling: Leveraging context provided by large, data sets for predictive vulnerability analysis, resilience modeling, and intrusion tolerance for a wide variety of integrated systems including IT, grid, cyber-physical, remote sensing, etc. These capabilities will enable optimization and design of resilient cyber systems, robust learning of system state such as topology estimate and congestion profiles, and interdependent system assessment. These capabilities require investment and new science in core mixed-integer non-linear optimization, data-driven machine learning, and numerical methods for interconnected systems operating at vastly different spatio-temporal scales.
    - Adversarial artificial intelligence (AI): Developing strategies to counter human and automated attackers of increasing levels of technical sophistication through a deep understanding of adversarial dynamics developed from specialized test beds, analytical expertise, and knowledge of cyber operations,
- Sense-making and acting in mission-critical situations:
    - Operational Technology: LANL designs, builds, and operates a wide variety of computerized technologies for advanced manufacturing, additive manufacturing, industrial control systems, experiment control systems, building automation, power grid, wastewater, and other purposes.
    - Artificial Intelligence: Machine Learning & Statistics methods applied to anomalous change detection, user behavioral analysis, and insider threat mitigation.

Supporting Capabilities

- Software Prototyping and Engineering: The ability to deliver applied solutions that meet internal or external user expectations requires a level of system architecture and software engineering that ranges from prototyping to operationally-viable deliverables. This requirement includes computing infrastructure, workflows, and expertise.

- Testbed development and instrumentation: LANL has unique facilities that provide valuable insights for cyber-physical security. Properly instrumenting these facilities and storing the data in an accessible, reliable, and secure manner is of critical importance to support studies at all levels of classification enabling unique operational and R&D activities. LANL's existing network/netflow data pool is extensive, enduring, and constantly growing to facilitate research in the identified investment areas.

- Situational Awareness: Collection/inference/situational awareness/response; Sensing platforms in space, air, and on the ground; advanced sensing modalities, modality-specific data modeling, analytics modeling, knowledge modeling, and large-scale data management, as well as visualization, human computer interaction, and decision support sciences. Includes awareness of national-level priorities and emerging threats.

Next Steps

This strategy identifies LANL's strengths as they relate to cyber sciences and is intended to guide internal investments to increase the strength, focus, and impact of LANL's cyber capability building innovative scientific leadership. Subsequent documents (human capital development, implementation, capabilities, infrastructure, etc.) will develop plans targeting specific program areas including weapons, energy, and strategic partnership programs. Strategic focus in LANLs cyber capability will allow development of innovative scientific solutions to anticipate global cyber security threats and inform solutions that anticipate national security and science challenges.

Strategy Team

A: Matt Kirkland, Rebecca Pratt (Executor)
CCS: Aric Hagberg
CIO: Mike Fisk (Chair)
GS-IET: Dave DeCroix, Gina Fisk
GS-NSD: Scott White
ISR: Michael Cai
NIE: Mike Zollinger
P: Ray Newell
T: Jack Shlachter, Pieter Swart
WRS: Carla Breiner